

INFORMATION REWRITING PROCESS OF SMART CARD

Patent number: JP7110876
Publication date: 1995-04-25
Inventor: JIYANNKURODO PERE; ERITSUKU DEYUPURE;
 FUJITSUPU IOYU
Applicant: CENTRE NAT ETD TELECOMM; POSUTO
Classification:
 - international: G07F7/12
 - european: G07F7/02C; G07F7/08C; G07F7/08E4; G07F7/10D4E2;
 G07F7/10D12
Application number: JP19940077562 19940415
Priority number(s): FR19930004515 19930416

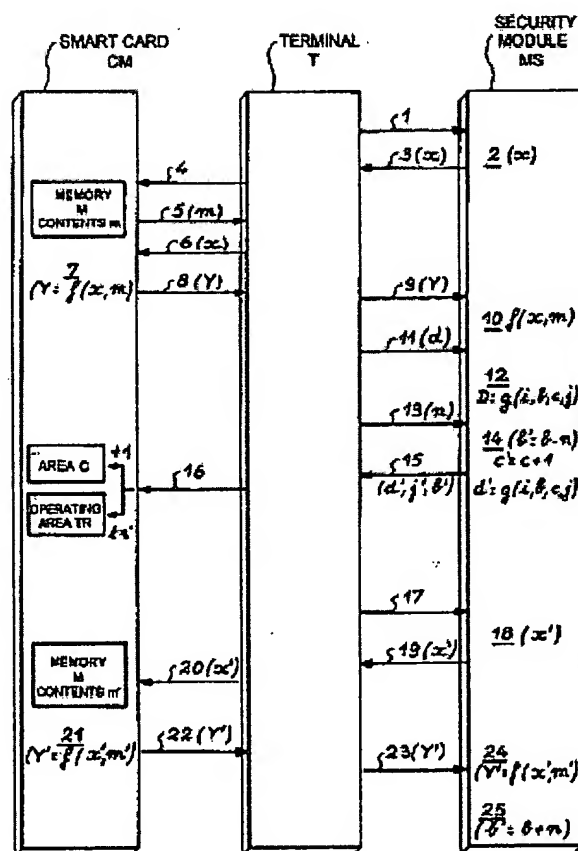
Also published as:

EP0621570 (A1)
 US5495098 (A1)
 FR2704081 (A1)
 EP0621570 (B1)

Report a data error here

Abstract of JP7110876

PURPOSE: To prevent the illegal use of a card such as transferring money larger than a paid amount from one card, for example.
CONSTITUTION: Concerning this information rewriting process for smart card, an operation for preventing the danger of illegal card usage is added to several operations provided by EP-A-423035. Namely, a memory (M) of the card has a certificate (d), namely, identification (i) of the card, the remainder (b) and prescribed function (g) related to contents (c) of a counter and before updating data, the counter is incremented for '1'. Besides, the certificate (d) is also functioned as a function related to identification (j) of a security module (MS) provided at a terminal.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-110876

(43) 公開日 平成7年(1995)4月25日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 7 F 7/12			G 0 7 F 7/ 08	C

審査請求 未請求 請求項の数 4 O L (全 5 頁)

(21) 出願番号	特願平6-77562	(71) 出願人	592057064 フランス・テレコム・エタブリセマン・オートノム・ドゥ・ドロワ・パブリック フランス・75015・パリ・プラス・ダレレイ・6
(22) 出願日	平成6年(1994)4月15日	(71) 出願人	594024774 ラ・ポスト フランス・92777・ブローニュ・ビランクール・セデックス・クアイ・デュ・プワ ン・デュ・ジュール・4
(31) 優先権主張番号	9 3 0 4 5 1 5	(74) 代理人	弁理士 志賀 正武 (外2名)
(32) 優先日	1993年4月16日		
(33) 優先権主張国	フランス (F R)		

最終頁に続く

(54) 【発明の名称】 スマートカードの情報書き換えプロセス

(57) 【要約】

【目的】 本発明によるスマートカードの情報書き換えプロセスは、たとえば1枚のカードから支払われた額以上を引き出させるようなカードの不正使用を防止する。

【構成】 本発明によるスマートカードの情報書き換えプロセスは、E P - A - 4 2 3 0 3 5 に開示されたいくつかの操作に加えることに、カード不正使用の危険を防止するための操作を追加している。すなわち、カードのメモリー (M) にカウンタと、認可証 (d) すなわちカードの同定 (i)、残高 (b)、およびカウンタの内容 (c) に係る所定の関数 (g) とを有しており、データ更新の前にはカウンタが1増分され、また認可証 (d) は、端末に備えられたセキュリティモジュール (MS) の同定 (j) に係る関数としても機能する。

にあるように、プリペイドカードにはセキュリティ上の問題がある。この問題は解放型の場合、つまり端末がカード発行機関に対して集金された金額の信頼性を証明する必要がある場合に、特に重要となる。その目的のために、各端末はセキュリティモジュールを備える必要がある。

【0004】このようなセキュリティ上の問題は、以下のような詐欺の危険を考慮すると、より鮮明となる。

【0005】危険(a)： 交換されたデータの改変：
カードとセキュリティモジュールとの間にデータ処理デ
バイスを介在させて、たとえば、カードから支払われた
以上の額をセキュリティモジュールに登録するように、
伝送されたデータを改変することができないようにして
おく必要がある。

【0006】危険(b)： 交換されたデータの再使用：
たとえば、カードからの1回の支払いを基礎にして同一
のセキュリティモジュールに対して複数回支払いを行な
うように、データ交換を反復させることを防がなくては
ならない。

【0007】危険(c)： 別のセキュリティモジュールの挿入：
第二のセキュリティモジュールを挿入して、1枚のカー
ドからの1回の支払いを基礎に、2つのセキュリティモ
ジュールに支払いを行なわせるようにすることが可能で
あってはならない。

【0008】危険(d)： カードの内容の改変：
カードの購買力を不法に増加すべくカードの内容を改変
することが可能であってはいない。

【0009】これらの問題を解決するには、様々なチェ
ック、データ操作(スクランプリング)、署名確認など
を行なうことのできるマイクロプロセッサをカードに導
入すればよい。

【0010】このような解決法は、ある面においては満
足のいくものであるが、各カードにマイクロプロセッサ
を導入しなければならないため、高価であるという不利
な点がある。

【0011】EP-A-423 035が開示する電子
スマートカードによる支払いまたは情報伝送システム
は、マイクロプロセッサの使用を排除している。このシ
ステムは様々な記憶領域をもち、そこには所有者同定情
報を持つ領域、認可証を持つ領域、カウンタを持つ領
域、残高情報を持つ領域、秘密コードを持つ領域があ
る。

【0012】カウンタは、カードによって行なわれる財
務操作の回数をカウントする。認可証は、所有者の同
定、カウンタの内容、および残高に係る関数である。

【0013】このシステムは、カードの不正使用を排除
することができないという意味で、セキュリティの問題
を完全に解決しているわけではない。つまり認可証およ

び残高情報をもつ領域は特に制限なしに消去して書き換
えることができる。従って、たとえば1枚のカードから
10点(10ユニット)分の支払いを行なって、2台の
端末に10点ずつの支払いをさせることによって、10
点分の不当な支払いを作り出すことは防止しようがな
い。

【0014】本発明の目的は、この欠点を除去すること
にある。

【0015】

【課題を解決するための手段】本発明は上記引用文献に
よって開示された操作のいくつか(カウンタのカウン
トアップ、認可証の作成)を採用しているが、その他
に、不当な支払いを偽造される危険を防止する操作を追
加している。認可証の計算にはセキュリティモジュール
の同定が前提となっており、同一のプリペイドカードに
よる同一の取引操作が2台の異なった端末から行なわれ
た場合、計算された二つの認可証が必ず異なるようにな
っている。更に、認可証を消去して書き換えるために
は、カウンタの値を一つアップする必要がある。最後
に、取引の前後に端末がプリペイドカードとその内容の
確認を行なう。

【0016】より詳しく述べると、本発明はスマートカ
ード(CM)に含まれたメモリー(M)の一部分(T
r)に含まれた情報(t r)をセキュリティモジュール
の備わった端末(T)によって更新するためのプロセス
に関する。メモリー(M)はカウンタ領域(C)を有
し、更新されるべきメモリー(M)の部分(T r)の内
容はその部分(T r)の一領域(D)に認可証(d)を
有する。この認可証とは、カードの同定(i)、別の領
域(B)に含まれる残高情報(b)、およびカウンタ領
域(C)の内容(c)に係る関数(g)である。前記プ
ロセスは、カウンタ領域(C)の内容(c)を1単位分
増加してから、メモリー(M)の部分(T r)の更新、
部分(T r)の旧内容を消去して、その代わりに新しい
更新された内容(t r')を入力する。また前記プロセ
スの特徴として、認可証(d)が、最終的更新を行な
ったセキュリティモジュール(MS)の同定(j)の関数
ともなっており、領域(D)に含まれる認可証を消去し
て更新された認可証に書き換えるには、更新の前後にカ
ウンタ領域(C)がカウントアップされ、端末(T)が
カード(CM)とその内容(m)を確認する。

【0017】カードの確認には、データ処理のセキュリ
ティ分野において伝統的手法であるチャレンジ・応答過
程が使用できる。端末がカードに、ランダムに選んだ値
あるいはすでに使用された値とは異なる値としてチャレ
ンジxを与えると、カードは次式を計算する。

$$Y = f(x, m)$$

式中、mはメモリーの内容を示す。次に端末はYをチェ
ックするために同じ計算を行なうことによって、カード
が本物であること、その内容が正しいことを確認するこ

1. TがMSにランダム変数を選択するよう依頼する。
2. MSがランダム変数つまり x を選択して記憶する。
3. MSが x をTへ転送する。
4. TがCMにメモリーMの内容を読むよう依頼する。
5. CMがMを読んで m をTに転送する。
6. TがCMにランダム変数 x を使用して自身(CM)を確認するよう依頼する。
7. CMが $Y = f(m, x)$ を計算する。
8. CMがTに Y を転送する。
9. TがMSに Y および m を転送する。
10. MSが $f(x, m)$ を計算して、 Y が本当に $f(x, m)$ に等しいことを確認する。
11. TがMSに認可証 d をチェックするよう依頼する。
12. MSが $D = g(i, b, c, j)$ を計算する。
13. TがMSに借り方を n にするよう連絡する。
14. MSが残高の新しい値 $d' = d - n$ を計算し、 c を $c' = c + 1$ にカウントアップして、 $d' = g(i, b', c', j')$ を計算する。
15. MSが更新された d', j', b' をTに転送する。
16. TがCMに依頼して、領域Cに1を書き込み、操作領域Trの内容 t_r を消去し、そこに j', b', d' から成る新しい内容を書き込ませる。
17. TがMSに新しいランダム変数を選択するよう依

頼する。

18. MSがランダム変数 x' を選択して記憶する。
19. MSが x' をTにアドレスする。
20. TがCMに、その新しい内容 m' によって自身を確認するよう依頼する。
21. CMが $Y' = f(x', m')$ を計算する。
22. CMがTに Y' の値を転送する。
23. TがMSに Y' の正当性をチェックさせる。
24. m' が i', c', j', b', d' に対応すること、および $Y' = f(x', m')$ であることをMSがチェックする。
25. 確認結果が正しければ、MSがその残高を n 分だけ増加させる。

【0026】先行する複数の操作により、カードの残高が減少し、端末によって集金される額が増加する。この一連の同じ操作が、カードに再度課金して残高を増やして課金する端末の方は同額分減らすことにも使用できることは明らかである。

【0027】上記例において、 (m) はカード(M)内のデータの内容を表わす。ただし、認可証(d)のデータおよび残高(b)のデータを (m) に含めないことも可能である。その場合、これらのデータは Y が(j)に係る関数である事実によって間接的に確認することができ、実施例の導入を簡素化できる。

フロントページの続き

(72)発明者 ジャンクロード・ベレ
フランス・14610・エブロン・リュ・デ
ルワシール・4

(72)発明者 エリック・デュブレ
フランス・14000・カン・リュ・ガリエイ
ニ・52

(72)発明者 フィリップ・イオユ
フランス・14200・エルーヴィユ・サン・
クレール・クアルティエール・グランド・
デル・1201